Theodore W. Maya (SBN 223242)
tmaya@ahdootwolfson.com
Alyssa Brown (SBN 301313)
abrown@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Ave. Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

Andrew W. Ferich (*pro hac vice* forthcoming)
AHDOOT & WOLFSON, P.C.
201 King of Prussia Road, Suite 650
Radnor, PA19087
Tel.: 310-474-9111
Facsimile: 310-474-8585
aferich@ahdootwolfson.com

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Fax: (865) 522-0049
Email: jnelson@milberg.com

Counsel for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SEDRE WRIGHT, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CROSSROADS TRADING CO., INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Sedre Wright ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant Crossroads Trading Co., Inc. ("Crossroads" or "Defendant") for its failure to properly safeguard sensitive personally identifiable information ("PII") stored within Defendant's information network. Plaintiff's allegations are based upon personal knowledge as to Plaintiff and Plaintiff's own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiff's attorneys.

INTRODUCTION

1. This class action arises out of the recent data breach (the "Data Breach") involving Crossroads, which collected and stored certain sensitive personal information ("Personal Information") of Plaintiff and Class members.

2. Crossroads is a retail business that buys, sells, and trades secondhand and vintage clothing items. During the course of its business, Crossroads collected certain Personal Information from Plaintiff and Class members. Crossroads owes a duty to the individuals for whom Crossroads obtains and maintains this data. This duty arises because it is foreseeable that the exposure of Personal Information to unauthorized persons, especially to perpetrators of cyberattacks with nefarious intentions, will result in harm to the affected individuals, including, but not limited to: the invasion of their private data, the sale of their Personal Information to facilitate identity theft, exposure to scams or phishing frauds, loss of time, economic damages as affected individuals scramble to protect their identities, and/or the countless ways these individuals' peace of mind is destroyed knowing their information is no longer secured.

3. Given the dire consequences of compromised Personal Information, individuals expect their data to be securely protected. Unfortunately, this trust is misplaced and violated when entities, like Defendant, subject themselves to the risk of cyberattacks.

4. Despite being aware that it was storing sensitive Personal Information that is valuable and vulnerable to cyberattackers, Crossroads failed to take basic security precautions that could have protected Plaintiff's and Class members' sensitive data.

5. As part of the Data Breach, at least the following sensitive PII of Plaintiff and Class members was disclosed and compromised: names, Social Security numbers (SSNs), driver's license numbers, and other government-issued identification ("ID") numbers.

6. Plaintiff and Class members have been victimized by the Data Breach and remain at a continuing and imminent threat of harm, as any combination of this Personal Information will forever subject them to being targets of fraud, identity theft, misuse, and other wrongdoings. Passport numbers, government/state-issued IDs, and SSNs cannot easily be changed.

7. The Data Breach was a direct result of Crossroads' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Personal Information. Specifically, Crossroads disregarded the rights of Plaintiff and Class members by (a) failing to take adequate and reasonable measures to ensure the security of its databases and information technology ("IT") systems; (b) concealing or otherwise omitting the material fact that it did not have systems in place to safeguard Personal Information; (c) failing to take available steps to detect and prevent the Data Breach; (d) failing to monitor its databases and IT systems and to timely detect the Data Breach; and (e) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

8. Due to Crossroads' inadequate security practices, negligence, and other data security shortcomings, affected Class members face a constant threat of repeated harm. Further, Class members face threats of crimes such as fraudulent opening of new financial accounts in Class members' names, taking out fraudulent loans, using Class members' information to obtain government benefits, filing fraudulent tax returns, and filing false medical claims.

9. Plaintiff and Class members retain a significant interest in ensuring that their Personal Information, which remains in Crossroads' possession, is protected from further breaches, and seek to remedy the harms suffered as a result of the Data Breach.

10. Plaintiff, individually, and on behalf of similarly situated persons, seeks to recover damages, equitable relief (including injunctive relief designed to prevent a reoccurrence of the Data Breach and resulting injuries), restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies deemed proper.

PARTIES

Plaintiff Sedre Wright

11. Plaintiff Sedre Wright is, and at all relevant times was, a California resident. Believing Crossroads would implement and maintain reasonable data security practices to protect customers' and other affiliated persons' Personal Information, Plaintiff provided Crossroads with Personal Information, or otherwise had Personal Information provided to Crossroads.

12. In March 2025, Plaintiff received a letter from Crossroads informing that Plaintiff was affected by the Data Breach and that his Personal Information was compromised in the Data Breach. The time spent dealing with the incidents resulting from the Data Breach is time Plaintiff otherwise would have spent on other activities, such as work and/or recreation. Plaintiff may have to take additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing accounts for any unauthorized activity.

13. Plaintiff reasonably expected that Crossroads would safeguard Personal Information. Plaintiff would not have trusted Crossroads with Personal Information, or agreed to have Personal Information provided to Crossroads, if Plaintiff knew that the information collected by Crossroads would be at risk. Plaintiff has suffered irreparable damage and has been placed at a heightened risk of fraud or identity theft as a result of the Data Breach.

Defendant Crossroads Trading Co., Inc.

14. Crossroads Trading Co., Inc., is corporation organized and existing under the laws of the State of California.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), there are in excess of 100 Class members, the action is a class action in which one or more Class members are citizens of states different from Defendant, and Defendant is not a government entity.

16. The Court has personal jurisdiction over Defendant because Defendant has a principal place of business in Berkeley, California, operates in California, conducts other significant business

in California, and otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in California.

17. Venue properly lies in this judicial district because, *inter alia,* Defendant has a principal place of business in this district; Defendant transacts substantial business, has agents, and is otherwise located in this district; and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this judicial district.

FACTUAL ALLEGATIONS

A. OVERVIEW OF CROSSROADS

18. Crossroads Trading Co., Inc., is a Berkeley, California-based retailer that buys, sells, and trades secondhand and vintage clothing items. It operates multiple store locations throughout the United States and specializes in curating pre-owned clothing and accessories from various contemporary and designer brands.

19. In the regular course of its business, Crossroads collects and maintains the PII of customers, employees, and other persons who otherwise are affiliated or transacted with Crossroads for business purposes.

20. Crossroads requires customers and other affiliated persons to provide their highly sensitive PII as part of its business operations, including names, SSNs, and driver's license numbers or other state ID numbers. Crossroads stores this information digitally.

21. In collecting and maintaining PII, Crossroads implicitly agreed to safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

22. Crossroads implicit promise to protect data privacy is embedded in its Privacy Policy.[1]

23. Despite a tacit acknowledgment of its duty to do so, Crossroads has not implemented reasonable cybersecurity safeguards or policies to protect consumers' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Crossroads has significant vulnerabilities in its systems that cybercriminals can exploit to gain access to consumers' PII.

[1] *Privacy Policy*, CROSSROADS, https://crossroadstrading.com/privacy-policy/ (last visited Apr. 2, 2025).

24. By obtaining, collecting, using, and benefitting from Plaintiff's and class member's PII, Defendant assumed legal and equitable duties that required Defendant to, at a minimum, implement adequate safeguards to prevent unauthorized use or disclosure of PII and to report any unauthorized use or disclosure of PII.

25. Plaintiff and Class members are, or were, customers or employees of Defendant, or otherwise are affiliated or transacted with Defendant, and entrusted Defendant with their PII.

26. Plaintiff and Class members reasonably relied on Defendant to maintain the confidentiality and security of their PII and to only make the required, authorized disclosures of this information, which Defendant ultimately failed to do.

B. THE DATA BREACH

27. On or about February 15, 2025, Crossroads discovered that an unauthorized third party had gained access to Crossroads' network systems.

28. Over a month later, on or about March 26, 2025, Crossroads began sending letters notifying customers of the Data Breach (the "Notice Letters"). The Notice Letters that Crossroads sent to Plaintiff and the class stated that "an unauthorized third-party gained access to our server and encrypted data stored on the Company's network." Crossroads determined that the systems accessed included systems that stored PII, including names, SSNs, and driver's license information and other state ID numbers.

29. Crossroads' Notice Letter omits pertinent information, including how criminals gained access to the encrypted files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, how it determined that the PII had been accessed, and of particular importance to Plaintiff and Class members, what actual steps Crossroads took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks. To date, these omitted details have not been explained or clarified to Plaintiff and Class members, who retain a vested interest in ensuring that their PII remains protected.

30. Based on Crossroads' acknowledgment that "an unauthorized third-party gained access to [its] server and encrypted data stored on the Company's network," it is evident that unauthorized criminal actors did, in fact, access Crossroads' network and exfiltrate Plaintiff's and

Class members' PII in an attack designed to acquire that sensitive, confidential, and valuable information.

31. Public reporting indicates that the ransomware group called Qilin has claimed responsibility for or is otherwise identified as responsible for the Data Breach.[2] Ransomware groups like Qilin carry out data breaches and cyberattacks with the sole purpose of monetizing the data stolen, meaning that Plaintiff's and Class members' Personal Information is at risk of misuse indefinitely.

C. CROSSROADS FAILED TO FOLLOW FTC GUIDELINES

32. According to the Federal Trade Commission (the "FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has promulgated numerous guides for businesses, which highlight the importance of implementing reasonable data security practices.

33. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

34. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.

35. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

36. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is

[2] *Crossroads Trading Data Breach*, BREACHSENSE.COM, https://www.breachsense.com/breaches/crossroads-trading-data-breach/ ; *[QILIN] – Ransomware Victim: Crossroads Trading Company, Inc.,* REDPACKETSECURITY.COM, https://www.redpacketsecurity.com/qilin-ransomware-victim-crossroads-trading-company-inc/ (last visited Apr. 2, 2025).

attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[3]

37. The FTC further recommends that companies not maintain the PII of customers for longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

38. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations. These FTC enforcement actions include actions against retailers, like Defendant.

39. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

40. Defendant was at all times fully aware of its obligation to protect the PII it was entrusted with. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class members.

[3] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

D. CROSSROADS FAILED TO COMPLY WITH INDUSTRY STANDARDS FOR DATA SECURITY

41. Experts studying cybersecurity routinely identify corporations—especially retailers—as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

42. Several best practices have been identified that, at a minimum, should be implemented by corporate entities like Defendant, including, but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

43. Other standard best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

44. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

45. These foregoing frameworks are existing and applicable industry standards in the corporate industry and Defendant failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

/ / /

/ / /

/ / /

/ / /

E. CROSSROADS OWED PLAINTIFF AND CLASS MEMBERS A DUTY TO SAFEGUARD PII

46. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class members.

47. Defendant owed a duty to Plaintiff and Class members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

48. Defendant owed a duty to Plaintiff and Class members to implement processes that would detect a compromise of PII in a timely manner.

49. Defendant owed a duty to Plaintiff and Class members to act upon data security warnings and alerts in a timely fashion.

50. Defendant owed a duty to Plaintiff and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

51. Defendant owed a duty of care to Plaintiff and Class members because they were the foreseeable and probable victims of any inadequate data security practices.

F. CROSSROADS KNEW THAT CRIMINALS TARGET PII

52. It is well known that PII, including SSNs, is an invaluable commodity and a frequent target of hackers. Data breaches, including those perpetrated against retailers that store PII in their systems, have become widespread.

/ / /

/ / /

/ / /

53. In the third quarter of the 2023 fiscal year alone, 733 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[4]

54. Additionally, as companies became more dependent on computer systems to run their businesses, e.g., working remotely as a result of the COVID-19 pandemic, and the Internet of Things, the danger posed by cybercriminals magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[5]

55. Indeed, cyberattacks have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[6]

56. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[7]

57. The Office for Civil Rights ("OCR") urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, OCR's deputy director of health

---

[4] *See ITRC Q3 Data Breach Analysis*, IDENTITY THEFT RESOURCE CENTER (2023), https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed July 16, 2024).

[5] Suleyman Ozarslan, *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, PICUS SECURITY (Mar. 24, 2022), https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.

[6] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[7] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[8]

58. In April 2020, ZDNet reported, in an article titled "*Ransomware mentioned in 1000+ SEC filings over the past year*," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[9]

59. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published an online "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[10]

60. In light of these warnings, and the recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII it collected and maintained would be targeted by cybercriminals.

61. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of PII preceding the date of the breach.

62. At all relevant times, Defendant knew, or should have known, that Plaintiff's and all other Class members' PII was a target for malicious actors. Despite such knowledge, Defendant

---

[8] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, (Apr. 22, 2014), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/concentra-health-services/index.html

[9] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNET (Apr. 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/.

[10] *Ransomware Guide*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (Sept. 2020), https://www.cisa.gov/sites/default/files/2023-01/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyberattacks that Defendant should have anticipated and guarded against.

63. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII belonging to Crossroads' customers, employees, and other affiliated persons, such as Plaintiff and Class members.

G. PII IS INHERENTLY VALUABLE

64. PII is a valuable property right.[11] The value of PII as a commodity is measurable.[12] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[13] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[14] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black market," or the "dark web," for many years.

65. As a result of its real value and recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, SSNs, PII, and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

---

[11] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY (May 2015), https://www.researchgate.net/publication/283668023 ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible ....").

[12] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE MEDICAL NEWS (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[13] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, at 4, OECD Publishing, Paris (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[14] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, Interactive Advertising Bureau (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

66. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.

67. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[16] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[17] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[18] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[19]

68. Consumers place a high value on the privacy of their data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[20]

---

[15] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[16] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[17] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[18] *In the Dark*, VPNOVERVIEW.COM, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited on Apr. 2, 2025).

[19] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI Cyber Division Private Industry Notification (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[20] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

69. Further, an active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[21]

70. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who, in turn, aggregates the information and provides it to marketers or app developers.[22]

71. As a result of the Data Breach, Plaintiff's and Class members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

72. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

H. THEFT OF PII HAS GRAVE AND LASTING CONSEQUENCES FOR VICTIMS

73. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[23]

74. Identity thieves use PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[24] Experian, one of the largest credit reporting companies in

[21] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[22] David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, LOS ANGELES TIMES (Nov. 5, 2019 5:00 AM PT), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[23] *See What to Know About Identity Theft*, Federal Trade Commission Consumer Advice, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last visited Apr. 2, 2025).
[24] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social

the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[25]

75. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[26]

76. Moreover, SSNs are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's SSN, as experienced by Plaintiff and Class members, can lead to identity theft and extensive financial fraud:

> Scammers use your Social Security Number (SSN) to get other personal information about you. They can use your SSN and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your SSN until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.[27]

77. It is no easy task to change or cancel a stolen SSN. An individual cannot obtain a new SSN without significant paperwork and evidence of actual misuse. In other words, preventive action

---

security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[25] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[26] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMM'N, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Apr. 2, 2025).

[27] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 2, 2025).

to defend against the possibility of misuse of a SSN is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

78. Even then, a new SSN may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

79. Each year, identity theft causes billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes SSNs, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification (and sell them to criminals or undocumented immigrants), steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class members.

80. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on dark web black markets for years.

81. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

82. The PII exposed in this Data Breach—including names in combination with SSNs and driver's license and other state ID numbers—is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyberthieves get access to a person's highly sensitive information, they will use it.[29]

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-shackers-has-millionsworrying-about-identity-theft.

[29] Ari Lazarus, *How fast will identity thieves use stolen info?*, FEDERAL TRADE COMM'N BLOG (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

83. For instance, with a stolen SSN, which is only one subset of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[30]

84. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

85. One such example of criminals using PII for profit is the development of "Fullz" packages. Cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

86. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cybercriminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

87. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[31]

88. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach

[30] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number* USA TODAY (Nov. 15, 2017 4 PM ET), https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/.

[31] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/.

victim has to demonstrate ongoing harm from misuse of their SSN, and a new SSN will not be provided until after the victim has suffered the harm.

89. Due to the highly sensitive nature of SSNs, theft of the numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Jim Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[32]

90. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their SSN was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

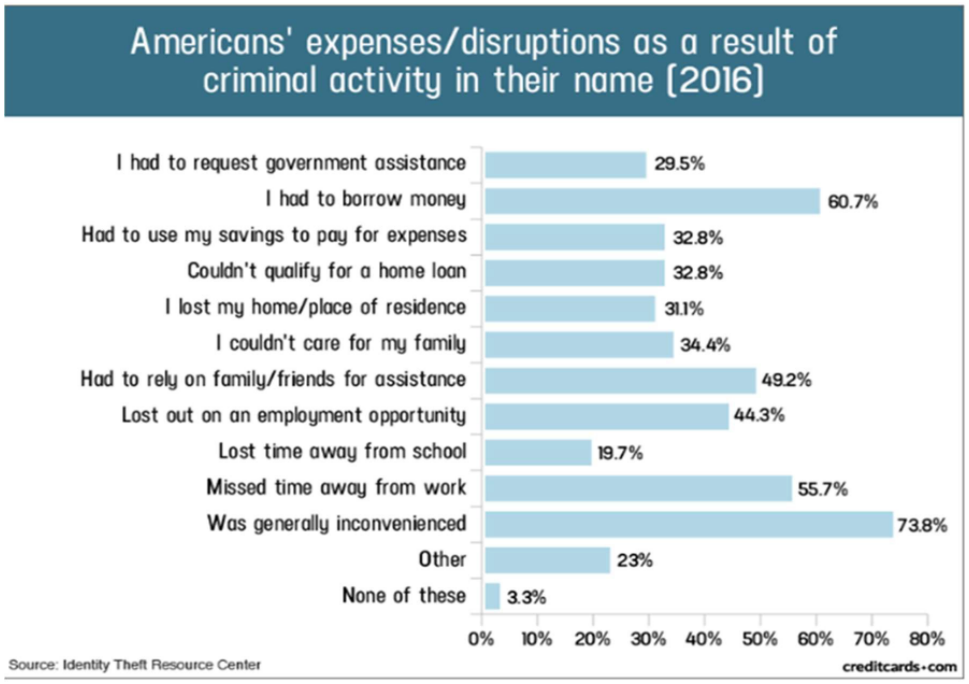
91. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[33]

92. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

93. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:

[32] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019 3:39 PM ET), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[33] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.



94. Victims of the Data Breach, like Plaintiff and Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[34]

95. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other account information for unauthorized activity for years to come.

96. Plaintiff and Class members have suffered or will suffer actual harms for which they are entitled to compensation, including, but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

[34] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMM'N, at 4 (Sept. 2013), http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential PII used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' PII for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

97. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown to be incapable of protecting Plaintiff's and Class members' PII.

I. THE DATA BREACH WAS FORESEEABLE AND PREVENTABLE

98. Data disclosures and data breaches are preventable.[35] As Lucy Thomson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of

[35] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thomson, ed., 2012).

appropriate security solutions."[36] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[37]

99. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[38]

100. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[39]

101. Plaintiff and Class members entrusted their PII to Defendant as a condition of transacting with Defendant. Plaintiff and Class members understood and expected that Defendant or anyone in Defendant's position would safeguard their PII against cyberattacks, delete or destroy PII that Defendant was no longer required to maintain, and timely and accurately notify them if their PII was compromised.

J. DAMAGES SUSTAINED BY PLAINTIFF AND CLASS MEMBERS

102. To date, Defendant has done nothing to provide Plaintiff and Class members with relief for the damages they have suffered as a result of the Data Breach. Crossroads only has offered two years of an Experian identity protection product. Not only did Defendant fail to provide adequate ongoing credit monitoring or identity protection services for individuals impacted by the Data Breach, but the credit monitoring identity theft protection services do nothing to compensate Class members for damages incurred and time spent dealing with the Data Breach.

103. Plaintiff and Class members have been damaged by the compromise of their PII in the Data Breach.

---

[36] *Id.* at 17.
[37] *Id.* at 28.
[38] *Id.*
[39] *See How to Protect Your Networks from RANSOMWARE*, at 3, FBI.GOV, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Apr. 2, 2025).

104. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and class members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

105. Plaintiff and Class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII, as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class members.

106. Plaintiff and Class members have and will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

107. Plaintiff and Class members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions and/or government agencies to dispute unauthorized and fraudulent activity in their names;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring SSNs, insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

108. Plaintiff and Class members suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their PII, a form of property that Crossroads obtained from Plaintiff and Class members;

(b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

109. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the resource and asset of time has been lost.

110. Plaintiff and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, researching online how to protect themselves from fraud and identity theft, signing up for the credit monitoring and identity theft insurance services offered by Defendant, contacting law enforcement regarding suspicious calls, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

111. Plaintiff's mitigation efforts are consistent with the steps that the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[40]

112. Class members who experience actual identity theft and fraud will need to spend time and money fixing the problem and repairing their good name.

113. Further, as a result of Defendant's conduct, Plaintiff and Class members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

[40] *See What To Do Right Away*, FED. TRADE COMM'N, https://www.identitytheft.gov/Steps (last visited Apr. 2, 2025).

114. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

115. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing PII is not accessible online, is properly encrypted, and that access to such data is password protected.

116. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cybersecurity training, procedures and protocols that were necessary to protect Plaintiff's and Class members' PII.

117. Defendant maintained the PII in an objectively reckless manner, making the PII vulnerable to unauthorized disclosure.

118. Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would result if Plaintiff's and Class members' PII were stolen, including the significant costs that would be placed on Plaintiff and Class members as a result of the breach.

119. The risk of improper disclosure of Plaintiff's and Class members' PII was a known risk to Defendant, and Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class members' PII from that risk left the PII in a dangerous condition.

120. Defendant disregarded the rights of Plaintiff and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an

unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

121. Plaintiff brings this action on own behalf of herself and the classes defined below, pursuant to Federal Rule of Civil Procedure 23(a) and (b):

> **Nationwide Class**
> All residents of the United States whose PII was or may have been affected in the Data Breach, including all persons who received a notice of the Data Breach.
>
> **California Class**
> All residents of California whose PII was or may have been affected in the Data Breach, including all persons who received a notice of the Data Breach.

122. The classes above are referred to as the "Class."

123. All members of the proposed Class are readily ascertainable. Defendant has access to the Class members' names and addresses affected by the Data Breach.

124. Excluded from the Class are: Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

125. Plaintiff reserves the right to amend or propose additional classes or subclasses upon conducting discovery.

126. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3), and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

127. **Numerosity**: The members of the Class are so numerous that joinder of all of them is impracticable. On information and belief, many tens of thousands of members comprise the Class.

128. **Commonality**: There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

- if Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class members' Personal Information;
- if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- if Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- if Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- if Defendant owed a duty to Class members to safeguard their Personal Information;
- if Defendant breached its duty to Class members to safeguard their Personal Information;
- if Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- if Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's misconduct;
- if Defendant's conduct was negligent;
- if Defendant breached implied contracts with Plaintiff and Class members;
- if Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class members;
- if Defendant failed to provide notice of the Data Breach in a timely manner; and
- if Plaintiff and Class members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

129. **Typicality**: Plaintiff's claims are typical of those of other Class members because Plaintiff's information, like that of every other Class member, was compromised in the Data Breach.

130. **Adequacy of Representation**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's counsel are competent and experienced in litigating class actions.

131. **Predominance**: Defendant has engaged in a common course of conduct toward Plaintiff and Class members, in that Plaintiff's and Class members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from

Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

132. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most members of the Class would likely find that the cost of litigating their individual claims is prohibitively high and they would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

133. **Declaratory and Injunctive Relief**: In addition, Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Federal Rule of Civil Procedure 23(b)(2). Defendant continues to: (1) maintain the PII of Class members; (2) fail to adequately protect Class members' PII; and (3) violate Class members' rights per the claims alleged herein. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

134. Plaintiff re-alleges and incorporates by reference all other paragraphs of this complaint as though fully set forth herein.

135. Plaintiff and the Class entrusted Defendant with their Personal Information on the premise and with the understanding that Defendant would safeguard their information, use their

Personal Information for limited business purposes only, and/or not disclose their Personal Information to unauthorized third parties.

136. Defendant has full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiff and the Class could and would suffer if the Personal Information were wrongfully disclosed.

137. Defendant has a duty to Plaintiff and Class members to safeguard and protect their Personal Information.

138. Defendant has a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with Personal Information data.

139. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class members' Personal Information held within it—to prevent disclosure of the information, and to safeguard the information. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

140. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and all other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

141. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and individuals who entrusted them with Personal Information, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

142. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

143. Defendant breached its duty of care by failing to secure and safeguard the Personal

Information of Plaintiff and Class members. Defendant negligently stored and/or maintained its data security systems and published that information on the internet.

144. Further, Defendant by and through its above negligent actions and/or inactions, breached its duties to Plaintiff and Class members by failing to design, adopt, implement, control, manage, monitor, and audit its processes, controls, policies, procedures, and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class members' Personal Information within its possession, custody, and control.

145. Pursuant to the FTC Act, Defendant had a duty to provide adequate data security practices in connection with safeguarding Plaintiff's and Class members' Personal Information.

146. Defendant breached its duties to Plaintiff and Class members under the FTC Act, the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et seq*. ("CCPA"), Cal. Civ. Code §§ 1798.80, *et seq*., the Consumers Legal Remedies Act, the Customer Record's Act, among other statutes, by failing to provide fair, reasonable, or adequate data security in connection with the sale of lending products and services in order to safeguard Plaintiff's and Class members' Personal Information.

147. Plaintiff and the other Class members have suffered harm as a result of Defendant's negligence. These victims' loss of control over the compromised Personal Information subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either the use of the compromised information or access to their user accounts.

148. It was reasonably foreseeable—in that Defendant knew or should have known—that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' Personal Information would result in its release and disclosure to unauthorized third parties who, in turn, wrongfully used such Personal Information, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

149. But for Defendant's negligent and wrongful breach of its responsibilities and duties owed to Plaintiff and Class members, their Personal Information would not have been compromised.

150. As a direct and proximate result of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of

Plaintiff's and Class members' Personal Information, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm for which they are entitled to compensation. Defendant's wrongful actions, inactions, and omissions constituted (and continues to constitute) common law negligence.

151. Plaintiff and Class members are entitled to injunctive relief as well as actual and punitive damages.

SECOND CAUSE OF ACTION.
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

152. Plaintiff re-alleges and incorporates by reference all other paragraphs of this complaint as though fully set forth herein.

153. Plaintiff and Class members formed an implied contract with Defendant regarding the provision of Defendant's services and through transacting business with it, including by Plaintiff and Class members providing their Personal Information to Defendant in exchange for the services offered.

154. Through Defendant's services, it knew or should have known that it needed to protect Plaintiff's and Class members' confidential Personal Information in accordance with their own policies, practices, and applicable state and federal law.

155. As consideration, Plaintiff and Class members turned over valuable Personal Information to Defendant, relying on Defendant to securely maintain and store their Personal Information in return for, and in connection with, Defendant's services.

156. Defendant accepted possession of Plaintiff's and Class members' Personal Information for the purpose of providing its services, including data security, to Plaintiff and Class members.

157. In delivering their Personal Information to Defendant in exchange for services, Plaintiff and Class members intended and understood that Defendant would adequately safeguard their Personal Information as part of those services.

158. Defendant's implied promises to Plaintiff and Class members includes, but is not limited to: (1) taking steps to ensure that anyone who is granted access to Personal Information, including its business associates, vendors, and/or suppliers, also protects the confidentiality of that data; (2) taking steps to ensure that the Personal Information that is placed in the control of its business associates, vendors, and/or suppliers is restricted and limited to achieve an authorized business purpose; (3) restricting access to Personal Information to qualified and trained employees, business associates, vendors, and/or suppliers; (4) designating and implementing appropriate retention policies to protect the Personal Information against criminal data breaches; (5) applying or requiring proper encryption; and (6) taking other steps to protect against foreseeable data breaches.

159. Plaintiff and Class members would not have entrusted their Personal Information to Defendant in the absence of such an implied contract.

160. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate data security and data supervisory practices to ensure the security of their sensitive data, including, but not limited to, Defendant's decision to continue to collect, store, and maintain Plaintiff's and Class members' Personal Information despite knowledge of Defendant's previous data breach, Plaintiff and Class members would not have agreed to provide their Personal Information to Defendant.

161. As a corporate retailer, Defendant recognized (or should have recognized) that Plaintiff's and Class member's Personal Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and the Class.

162. A meeting of the minds occurred, and an implied contract was formed, as Plaintiff and Class members agreed to, *inter alia*, provide their accurate and complete sensitive personal information to Defendant in exchange for Defendant's agreement to, *inter alia*, protect their Personal Information.

163. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures and supervision of its systems and networks, as well as its vendors, business associates, and/or suppliers, to secure Plaintiff's and Class members' Personal Information.

164. Plaintiff and Class members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

165. Accordingly, Plaintiff and Class members have been injured by Defendant's breach of contract and are entitled to damages, including nominal damages, and/or restitution in an amount to be proven at trial.

THIRD CAUSE OF ACTION

VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT CALIFORNIA CIVIL CODE § 1798.150 (On Behalf of Plaintiff and the California Class)

166. Plaintiff re-alleges and incorporates by reference all other paragraphs of this complaint as though fully set forth herein.

167. Plaintiff brings this claim individually and behalf of the California Class.

168. Cal. Civ. Code § 1798.150(a) of the California Consumer Privacy Act ("CCPA") provides that "[a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action" for statutory damages, actual damages, injunctive relief, declaratory relief and any other relief the court deems proper.

169. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Personal Information of Plaintiff and the California Class. As a direct and proximate result, Plaintiff's and the California Class's nonencrypted and nonredacted Personal Information was subject to unauthorized access and exfiltration, theft, or disclosure.

170. Defendant is a "business" under the meaning of Cal. Civ. Code § 1798.140 because Defendant is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal

information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Cal. Civ. Code § 1798.140(d).

171. Plaintiff and California Class members are "consumers" as defined by Cal. Civ. Code § 1798.140(g) because they are natural persons who reside in California.

172. Plaintiff and California Class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Personal Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Personal Information, including Plaintiff's and Class members' Personal Information.

173. Plaintiff and California Class members have an interest in ensuring that their Personal Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

174. Defendant has failed to take sufficient and reasonable measures to safeguard its data security systems and protect Plaintiff's and California Class members' highly sensitive Personal Information from unauthorized access. Defendant's failure to maintain adequate data protections subjected Plaintiff's and the California Class members' nonencrypted and nonredacted sensitive Personal Information to exfiltration and disclosure by malevolent actors.

175. The unauthorized access, exfiltration, theft, and disclosure of Plaintiff's and the California Class members' Personal Information was a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Personal Information.

176. Under Defendant's duty to protect customers' Personal Information, it was required to implement reasonable security measures to prevent and deter hackers from accessing the Personal Information of its customers. These vulnerabilities existed and enabled unauthorized third parties to access and harvest customers' Personal Information, evidence that Defendant has breached that duty.

177. Plaintiff and California Subclass members have suffered actual injury.

178. Defendant's violations of Cal. Civ. Code § 1798.150(a) are a direct and proximate result of the Data Breach.

179. Plaintiff sent Defendant notice consistent with the CCPA on or before April 2, 2024. If Defendant does not timely cure its violations of the CCPA, Plaintiff, individually and on behalf of the California Class, will amend this pleading to seek all monetary relief allowed under the CCPA and by law, including actual or nominal damages, reasonable attorneys' fees, and costs. At this time, Plaintiff seeks only non-monetary relief, including declaratory and injunctive relief, and an order barring Defendant from disclosing Personal Information without Plaintiff's and California Class members' consent.

FOURTH CAUSE OF ACTION
VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW
CAL. BUS. & PROF. CODE § 17200, *ET SEQ.* ("UCL")
(On Behalf of Plaintiff and the California Class)

180. Plaintiff re-alleges and incorporates by reference all other paragraphs of this complaint as though fully set forth herein.

181. Plaintiff brings this claim individually and on behalf of the California Class.

182. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

183. By reason of Defendant's above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiff's and Class members' Personal Information, Defendant engaged in unfair and unlawful business practices in violation of the UCL.

184. The acts, omissions, and conduct complained of herein in violation of the UCL were designed and emanated from Defendant's California corporate office.

185. Plaintiff suffered injury in fact and lost money or property as a result of Defendant's alleged violations of the UCL.

/ / /

/ / /

186. The acts, omissions, and conduct of Defendant as alleged herein constitute a "business practice" within the meaning of the UCL.

Unlawful Prong

187. Defendant violated the unlawful prong of the UCL by violating, *inter alia*, the CCPA and FTC Act as alleged herein.

188. Defendant violated the unlawful prong of the UCL by failing to honor the terms of its implied contracts with Plaintiff and Class members, as alleged herein.

189. Defendant's conduct also undermines California public policy—as reflected in statutes like the California Information Practices Act, Cal. Civ. Code §§ 1798, *et seq*., the CCPA concerning consumer privacy, and the CCRA concerning customer records—which seek to protect customer and consumer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

Unfair Prong

190. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because Defendant's acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and other Class members. The gravity of Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendant's conduct described herein.

191. Defendant's failure to utilize, and to disclose that it does not utilize, industry standard security practices, constitutes an unfair business practice under the UCL. Defendant's conduct is unethical, unscrupulous, and substantially injurious to the Class. While Defendant's competitors have spent the time and money necessary to appropriately safeguard their products, service, and customer information, Defendant has not—to the detriment of its customers and to competition.

192. As a result of Defendant's violations of the UCL, Plaintiff and Class members are entitled to injunctive relief including, but not limited to:

- ordering that Defendant utilize strong industry standard data security measures for the collection, storage, and retention of customer data;

- ordering that Defendant, consistent with industry standard practices, engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;
- ordering that Defendant engage third-party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring;
- ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
- ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems are compromised, hackers cannot gain access to other portions of those systems;
- ordering that Defendant purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its provisions of services;
- ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks;
- ordering that Defendant, consistent with industry standard practices, evaluate all software, systems, or programs utilized for collection and storage of sensitive Personal Information for vulnerabilities to prevent threats to customers;
- ordering that Defendant, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- ordering Defendant to meaningfully educate its customers about the threats they face as a result of the loss of their Personal Information.

193. As a result of Defendant's violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost money or property, as detailed herein. They agreed to transact with Defendant or made purchases or spent money that they otherwise would not have made or spent, had they known the true state of affairs regarding Defendant's data security policies. Class members

lost control over their Personal Information and suffered a corresponding diminution in value of that Personal Information, which is a property right. Class members lost money as a result of dealing with the fallout of, and attempting to mitigate harm arising from, the Data Breach.

194. Plaintiff requests that the Court issue sufficient equitable relief to restore Class members to the position they would have been in had Defendant not engaged in violations of the UCL, including by ordering restitution of all funds that Defendant may have acquired from Plaintiff and Class members as a result of those violations.

FIFTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Nationwide Class)

195. Plaintiff re-alleges and incorporates by reference all other paragraphs of this complaint as though fully set forth herein.

196. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

197. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

198. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the Personal Information it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

199. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its customers' (i.e., Plaintiff's and Class members') data.

200. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

201. An injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for judgment and relief on all cause of action as follows:

A. That the Court determines that this action may be maintained as a class action, that Plaintiff be appointed as Class Representative, that the undersigned be named as Class Counsel, and that notice of this action be given to Class members;

B. That the Court enter an order declaring that Defendant's actions, as set forth in this complaint, violate the laws set forth above;

C. That the Court issue an order:

- prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's utter failure to provide notice to all affected consumers);

- requiring Defendant to implement adequate security protocols and practices to protect consumers' Personal Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;
- mandating the proper notice be sent to all affected parties, and posted publicly;
- requiring Defendant to protect all data collected through its account creation requirements;
- requiring Defendant to delete, destroy, and purge the Personal Information of Plaintiff and Class members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members;
- requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiff's and Class members' Personal Information;
- requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;
- requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;
- requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;
- requiring Defendant to conduct systematic scanning for data breach related issues;
- requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the Personal Information data; and

/ / /

/ / /

- requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

D. That the Court award Plaintiff and the Class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

E. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiff and the Class are entitled, including, but not limited to, restitution and an order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

F. That the Court award Plaintiff and the Class pre- and post-judgment interest (including pursuant to statutory rates of interest set under state law);

G. That the Court award Plaintiff and the Class their reasonable attorneys' fees and costs of suit;

H. That the Court award treble and/or punitive damages insofar as they are allowed by applicable laws; and

I. That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

DATED: April 14, 2025

Respectfully submitted,

/s/ *Theodore W. Maya*

Theodore W. Maya (SBN 223242)
tmaya@ahdootwolfson.com
Alyssa Brown (SBN 301313)
abrown@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Ave. Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111
Facsimile: (310) 474-8585

Andrew W. Ferich (*pro hac vice* forthcoming)
AHDOOT & WOLFSON, P.C.
201 King of Prussia Road, Suite 650
Radnor, PA19087
Tel.: 310-474-9111

Facsimile: 310-474-8585
aferich@ahdootwolfson.com

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Fax: (865) 522-0049
Email: jnelson@milberg.com

Attorneys for Plaintiff and the Proposed Classes